

## CLAIMS

What is claimed is:

- 1 1. A computerized method to prevent identification of an operating system executing  
2 on a computer connected to a network comprising:  
3 intercepting a portion of outgoing network data characteristic of the operating  
4 system; and  
5 masking the portion of outgoing network data to impersonate a different operating  
6 system in accordance with a security policy if the network is an untrusted network.
- 1 2. The computerized method of claim 1, wherein masking the portion comprises:  
2 discarding the portion of outgoing network data.
- 1 3. The computerized method of claim 1, wherein masking the portion comprises:  
2 replacing the portion of outgoing network data with data characteristic of the  
3 different operating system.
- 1 4. The computerized method of claim 1, wherein the security policy identifies the  
2 portion of outgoing network data and specifies an action to take to mask the portion of  
3 outgoing network data.
- 1 5. The computerized method of claim 1, wherein the security policy further specifies  
2 replacement data for the portion of outgoing network data, the replacement data  
3 characteristic of the different operating system.
- 1 6. The computerized method of claim 1, wherein the security policy further defines  
2 the network as untrusted.

1 7. The computerized method of claim 1 further comprising:  
2 receiving the security policy through the network.

1 8. The computerized method of claim 1 further comprising:  
2 modifying the security policy based on user input.

1 9. The computerized method of claim 1 further comprising:  
2 transmitting the portion of outgoing network data unchanged if the network is a  
3 trusted network.

1 10. The computerized method of claim 1 further comprising:  
2 intercepting a portion of incoming network data; and  
3 sending a false response to the portion of incoming network data to impersonate  
4 the different operating system in accordance with the security policy if the network is an  
5 untrusted network.

1 11. The computerized method of claim 10, wherein the security policy identifies the  
2 portion of incoming network data and the false response.

1 12. The computerized method of claim 1, wherein the method is integrated into a  
2 firewall that protects the computer.

1 13. A computer-readable medium having executable instructions to cause a computer  
2 to perform a method comprising:

1 intercepting a portion of outgoing network data characteristic of an operating  
2 system executing on the computer when the computer is connected to a network; and  
3 masking the portion to impersonate a different operating system in accordance with  
4 a security policy if the network is an untrusted network.

1 14. The computer-readable medium of claim 13, wherein masking the portion  
2 comprises:  
3 discarding the portion.

1 15. The computer-readable medium of claim 13, wherein masking the portion  
2 comprises:  
3 replacing the portion with data characteristic of the different operating system.

1 16. The computer-readable medium of claim 13, wherein the security policy identifies  
2 the portion and specifies an action to take to mask the portion.

1 17. The computer-readable medium of claim 13, wherein the security policy further  
2 specifies replacement data for the portion, the replacement data characteristic of the  
3 different operating system.

1 18. The computer-readable medium of claim 13, wherein the security policy further  
2 defines the network as untrusted.

1 19. The computer-readable medium of claim 13, wherein the method further  
2 comprises:  
3 receiving the security policy through the network.

1 20. The computer-readable medium of claim 13, wherein the method further  
2 comprises:  
3 modifying the security policy based on user input.

1 21. The computer-readable medium of claim 13, wherein the method further  
2 comprises:

3 transmitting the portion unchanged if the network is a trusted network.

1 22. The computer-readable medium of claim 13, wherein the method further  
2 comprises:

3 intercepting a portion of incoming network data; and

4 sending a false response to the portion of incoming network data to impersonate  
5 the different operating system in accordance with the security policy if the network is an  
6 untrusted network.

1 23. The computer-readable medium of claim 22, wherein the security policy identifies  
2 the portion of incoming network data and the false response.

1 24. The computer-readable medium of claim 13, wherein the instructions are operable  
2 for integration into a firewall.

1 25. A computerized system comprising:  
2 a processing unit;  
3 a memory coupled to the processing unit through a bus;  
4 a network interface coupled to the processing unit through the bus and further  
5 operable for coupling to a network;  
6 an operating system executed from the memory by the processing unit; and  
7 a fingerprint masking process executed from the memory by the processing unit to  
8 cause the processing unit to intercept a portion of network data characteristic of the  
9 operating system when the network interface is coupled to the network, and to mask the  
10 portion to impersonate a different operating system in accordance with a security policy if  
11 the network is an untrusted network.

1 26. The computerized system of claim 25, wherein the fingerprint masking process  
2 further causes the processing unit to mask the portion by discarding the portion.

1 27. The computerized system of claim 25, wherein the fingerprint masking process  
2 further causes the processing unit to mask the portion by replacing the portion with data  
3 characteristic of the different operating system.

1 28. The computerized system of claim 25, wherein the fingerprint masking process  
2 further causes the processing unit to transmit the portion unchanged if the network is a  
3 trusted network.

1 29. The computerized system of claim 25, wherein the fingerprint masking process  
2 further causes the processing unit to receive the security policy through the network  
3 interface.

1 30. The computerized system of claim 25 further comprising a user input device  
2 coupled to the processing unit through the bus and wherein the fingerprint masking  
3 process further causes the processing unit to receive input through the user input device  
4 and to modify the security policy based on the input.

1 31. The computerized system of claim 25, wherein the fingerprint masking process  
2 further causes the processing unit to intercept a portion of incoming network data when the  
3 network interface is coupled to the network, and to send a false response to the portion of  
4 incoming network data to impersonate the different operating system in accordance with  
5 the security policy if the network is an untrusted network.

1 32. The computerized system of claim 25, wherein the fingerprint masking process is  
2 integrated into a firewall process that is executed by the processing unit.

1 33. The computerized system of claim 25, wherein the computerized system is a  
2 firewall and the fingerprint masking process masks an operating system on a computer  
3 coupled to the firewall.

1 34. A computer-readable medium having stored thereon an OS fingerprint policy data  
2 structure comprising:

3 a data unit type field containing data representative of an identifier for a type of  
4 data unit, wherein information associated with the data unit is characteristic of an  
5 operating system; and

6 an action field containing data representative of an action to be taken to mask the  
7 information associated with the data unit identified by the data unit type field.

1 35. The computer-readable medium of claim 34 further comprising:

2 a re-fingerprint field containing data representative of an identifier for a field type  
3 within the data unit type identified by the data unit type field, and further containing re-  
4 fingerprint data that identifies replacement data for the field identified by the field type.

1 36. The computer-readable medium of claim 35, wherein the re-fingerprint data is  
2 selected from the group consisting of the replacement data and a location for the  
3 replacement data.

1 37. The computer-readable medium of claim 34 further comprising:

2 a re-fingerprint field containing data representative of an identifier for a field type  
3 within a false response to the data unit type identified by the data unit type field, and  
4 further containing re-fingerprint data that identifies false data for the field identified by the  
5 field type.

